

KECCAK

Length Extension of KECCAK Cryptanalysis Prize

Guido BERTONI¹ Joan DAEMEN¹ Michaël PEETERS²
Gilles VAN ASSCHE¹

¹STMicroelectronics

²NXP Semiconductors

First SHA-3 candidate conference, Leuven, Belgium
February 28, 2009

Length Extension of KECCAK Cryptanalysis Prize

- **Prize...** is extended!
 - **25 bottles** of typical Belgian beers
- **Deadline...** is extended!
 - **Friday April 24, 2009 at KECCAK-f[1600] GMT+1**
- **What...**
 - Any **distinguisher** on KECCAK-*f*
 - ... See for instance Ch. 4 of KECCAK main document...
 - ... on **2-round, 3-round** reduced-version or more...
 - ... on **1-bit, 2-bit, 4-bit** version or more...
 - ... **The more the better!**



More information on
<http://keccak.noekeon.org/>

!!! Warning – too much consumption of the Prize may lead to strange cryptanalysis... !!!